IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI WESTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	**Case No. 15-00340-01-CR-W-GAF**
	)	
THOMAS JOHNSON,	)	
	)	
Defendant.	)	

ORDER

Presently before the Court is Defendant Thomas Johnson's ("Defendant's") Motion to Suppress Evidence. (Doc. # 26). On August 16, 2016, United States Magistrate Judge John T. Maughmer issued his Report and Recommendation ("R&R"). (Doc. # 40). On September 26, 2016, Defendant filed his Objections to the R&R. (Doc. # 43). For the reasons stated below, and upon careful and independent review of the pending motion, Defendant's objections to Judge Maughmer's R&R, as well as the applicable law, this Court hereby ADOPTS in part the R&R of Judge Maughmer and incorporates it in part as its own Opinion and Order and DENIES Defendant's Motion to Suppress Evidence. [1]

DISCUSSION

I. FACTS

The essential facts are agreed upon by the parties, which Judge Maughmer summarized as follows:

> On February 20, 2015, the federal government obtained an order from [] Magistrate Judge [Theresa Carroll Buchanan] in the United States District Court for the Eastern District of Virginia permitting the government to intercept

[1] The Court has reproduced the parts of Judge Maughmer's Report and Recommendations it adopts and incorporates as its own in its discussion.

communications by and between users of a particular global online forum ("Website A"). Website A is alleged to have been dedicated to the advertisement and distribution of child pornography. [Defendant] is alleged to be a frequent visitor to Website A.

Website A operated on what is sometimes referred to as the "dark web," and in the case of Website A, specifically on the Tor network. *See generally* www.torproject.org. Users of the Tor network must download special software that lets them access the network. One of the main characteristics of the Tor network is the seeming anonymity it affords to its users.

Typically, when an individual visits a website on the Internet, the website is able to determine the individual's Internet Protocol ("IP") address.[2] Because internet access is typically purchased for a single location, an IP address may be used by law enforcement to determine the home or business address of an Internet user. However, when an Internet user connects to a website, the only IP address that the website actually "sees" or "detects" is the IP address of the last computer through which the user's communications were routed ("the exit node"). When an Internet user accesses the Tor network, communications from that user are routed through a system of network computers that are run by volunteers around the world. As a consequence, because there is no practical way to trace a user's communications from the exit node back to the user's computer, Internet users of the Tor network are effectively anonymous to the websites and to law enforcement officers who may be monitoring the websites.[3]

Based on a tip from a foreign law enforcement agency and other investigation, the FBI determined that Website A was being hosted from a computer server at a web-hosting facility in North Carolina. Based on that information, in February of 2015, the FBI apprehended the administrator of Website A and seized the web site from the North Carolina web-hosting facility.

---

[2] An individual's IP address generally is associated with a particular Internet Service Provider ("ISP") and a particular ISP customer.

[3] The Tor network also provides anonymity to the individuals who run websites or forums on it. Websites may be set up on the Tor network as "hidden services" that may only be accessed through the Tor network. A hidden service functions much like a regular website except that its IP address is hidden and is replaced with a Tor-based address which consists of a series of alphanumeric characters followed by ".onion" (Tor is an acronym for "the onion router"). Thus, there is no way to look up the IP address of the computer hosting a hidden service. Moreover, in order even to access a hidden service, an Internet user must know the Tor-based address of the hidden service. As a result, an Internet user cannot simply stumble onto a hidden service. Instead, the user may obtain the address from postings on the Internet or by communications with other users of the Tor network. Often, one hidden service will also link to another. Website A was a hidden service contained on the Tor network, and it had been linked to by another hidden service that itself was also dedicated to child pornography.

> However, following the seizure, the FBI did not shut the site down. Instead, the FBI allowed the site to continue to operate from a government facility located in the Eastern District of Virginia from February 20 to March 4, 2015, simultaneously obtaining [Judge Buchanan's] order permitting it to intercept communications by and between users of Website A. The order, thus, allowed the government to employ a Network Investigative Technique ("NIT"). Specifically, the NIT search warrant allowed the government to include certain computer instructions in Website A's usual Tor access software. These computer instructions (a form of malware) caused a user's computer to transmit certain information (including a true IP address) so as to allow the FBI to identify and locate users of Website A. Using the information generated pursuant to the NIT warrant, the FBI determined that one particular IP address accessing Website A was associated with [Defendant's] residence.
>
> On September 24, 2015, law enforcement officers obtained a search warrant from a Magistrate Judge with this Court allowing a search of [Defendant's] residence. The search warrant was executed the next day. Subsequently a second search warrant was obtained to permit a search of the contents of a laptop allegedly belonging to [Defendant]. A forensic examination found child pornography on the laptop's hard drive. [Defendant] was then indicted for possession and production of child pornography as well as travel with intent to engage in illicit sexual conduct.

(R&R (located at Doc. # 40), pp. 1-3).

II. LEGAL STANDARD

"[T]he Federal Magistrates Act 'does not preclude further review [of a report and recommendation] by the district judge, *sua sponte* or at the request of a party, under a *de novo* or any other standard.'" *Streambend Prop. II, LLC v. Ivy Town Minneapolis, LLC*, 781 F.3d 1003, 1010 n.3 (8th Cir. 2015) (quoting *Thomas v. Arn*, 474 U.S. 140, 154 (1985)). However, when a party objects to the report and recommendation, in whole or in part, the district court judge must conduct a de novo review of it. 28 U.S.C. § 636(b)(1). "When conducting de novo review, the district court makes its own determinations of disputed issues . . . ." *Branch v. Martin*, 886 F.2d 1043, 1046 (8th Cir. 1989). The district court must undertake an independent and meaningful review of the evidence and law when conducting its de novo review. *United States v. Azure*, 539 F.3d 904, 910 (8th Cir. 2008). "The court need not conduct a de novo hearing, but must

nonetheless make a de novo determination of that finding based on the record." *Taylor v. Farrier*, 910 F.2d 518, 521 (8th Cir. 1990) (citations omitted). The Article III judge "may accept, reject, or modify, in whole or in part, the findings or recommendations made by the magistrate judge." 28 U.S.C. § 636(b)(1).

III. ANALYSIS

Defendant has raised six objections to Judge Maughmer's R&R: (1) the characterization that the Motion to Suppress was grounded solely on Federal Rule of Criminal Procedure 41(b); (2) the characterization that Defendant did not argue the officers intentionally or deliberately disregarded the provisions of Rule 41 when applying for and executing the NIT warrant; (3) that Defendant bore the burden to demonstrate prejudice; (4) the R&R does not analyze *United States v. Turner*, 781 F.3d 374 (8th Cir. 2015); (5) the conclusion that Defendant did not have a reasonable expectation of privacy in his IP address; and (6) the conclusion that the good-faith exception is applicable. (Doc. # 43, pp. 1-5). The Court has reviewed these objections and examined the evidence submitted to Judge Maughmer as well as the applicable law. For reasons discussed below, the Court overrules Defendant's objections and concludes the NIT warrant is valid, and alternatively, suppression of the evidence is not justified even if the warrant was invalid.

A. Validity of the NIT Warrant

Several cases in other districts have analyzed whether the NIT warrant issued by the Eastern District of Virginia was valid. Several courts have determined it was invalid but declined to suppress the evidence because the Rule 41 violation was only a technical or procedural violation. *See United States v. Adams*, No. 6:16-CR-11-Orl-40GJK, 2016 WL 4212079 (M.D. Fla. Aug. 10, 2016); *United States v. Acevedo–Lemus*, No. SACR15-00137-CJC,

2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *United States v. Werdene*, --F.Supp.3d--, 2016 WL 3002376 (E.D. Pa. May 18, 2016); *United States v. Epich*, No. 15-CR-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Stamper*, No. 1:15–CR–00109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016); *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). However, other courts have determined the NIT warrant was void *ab initio* and then suppressed the evidence. *See United States v. Croghan*, --F. Supp. 3d--, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016); *United States v. Levin*, --F. Supp. 3d--, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Arterbury*, No. 15–CR–182, slip op. (N.D. Okla. April 25, 2016). Still others have found the warrant is valid and declined to suppress the evidence. *See United States v. Jean*, --F. Supp. 3d--, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016); *United States v. Eure*, No. 2:16CR43, 2016 WL 4059663 (E.D. Va. July 28, 2016); *United States v. Darby*, --F. Supp. 3d--, 2016 WL 3189703 (E.D. Va. June 3, 2016); *United States v. Matish*, --F. Supp. 3d--, 2016 WL 3545776 (E.D. Va. June 23, 2016).

While the R&R followed the line of reasoning of the first group of cases, the Court is persuaded by the third group's analysis, particularly that of Judge Timothy L. Brooks in *Jean*. Judge Brooks's thorough and well-reasoned opinion first explored case law on the expectation of privacy, summarizing that, while the Eighth Circuit has never definitely ruled on the issue, the Third, Fourth, Sixth, Ninth, and Tenth have all explicitly held that there is no reasonable expectation of privacy in an IP address. *See Jean*, 2016 WL 4771096, at *8 (collecting cases). This is so because a person generally has no legitimate expectation of privacy in information he voluntarily turns over to third parties, *United States v. Miller*, 425 U.S. 435, 442-44 (1976), and IP addresses are regularly conveyed to and from third parties, including Internet service providers. *United States v. Christie*, 624 F.3d 558, 576 (3d Cir. 2010).

> The use of Tor software to mask a user's IP address does not change the analysis.
>
> TOR's encryption works by substituting components of the IP address of each volunteer node as it hops across the internet, but on its very first hop, the TOR user's true IP address is disclosed to the first node computer in the TOR chain. Thus, the user's true IP address is not a complete secret, and the user must necessarily assume some measure of risk that TOR's encryption technology could be defeated and thereby potentially reveal his true IP address. Taking this reasoning to its logical conclusion, the principles behind the decision in *United States v. Miller* would apply: If a user engaged in illegal activity while using TOR, and law enforcement obtained the user's true IP address, it would follow that the user would have no legitimate expectation of privacy in the IP address, as he "[took] the risk, in revealing his affairs to others,"—namely, to both his ISP and the owner of the first node computer in the TOR chain—"that the information [would] be conveyed by that person to the Government." 425 U.S. at 443, 96 S.Ct. 1619.

Jean, 2016 WL 4771096, at *9. Consequently, it is likely a warrant was not even constitutionally necessary to discover Defendant's IP address. *Id.* However, the fact is the FBI did obtain a warrant. Like Judge Brooks, the Court will assume a warrant was necessary as no definitive, binding authority on the matter currently exists.

In his objections to the R&R, Defendant contends Judge Maughmer did not address his Fourth Amendment argument concerning the NIT warrant. (Doc. # 43, ¶ 1). While the Court does not believe Defendant properly raised the issue in his Motion to Suppress because it was raised for the first time in his Reply suggestions to the Motion to Suppress, it will briefly address the issue as the NIT warrant fully complied with the Fourth Amendment requirements. Defendant asserted that, because the NIT warrant was invalid, the search of his computer is presumptively unreasonable. (Doc. # 33, p. 12). Specifically, he argued the warrant violated his expectation of privacy and was therefore invalid. As noted previously, Defendant had no expectation in the privacy in his IP address, even when using the Tor network. Consequently, the NIT warrant, having probable cause and sufficient particularity, meets the requirements of Fourth Amendment.

In the Motion to Suppress, Defendant primarily argued the NIT warrant violated Rule 41(b),[4] which provides:

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> (3) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
>
> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
>
> (A) a United States territory, possession, or commonwealth;
>
> (B) the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

[4] Defendant also sought suppression of evidence pursuant to 28 U.S.C. § 636(a), which provides that a magistrate judge shall have "all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts." Because § 636(a) encompasses the Federal Rules of Criminal Procedure, the Court considers Defendant's §636(a) argument intertwined with his Rule 41(b) argument and addresses them concurrently.

> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b). The Court disagrees with Defendant's argument, and agrees with Judge Brooks's analysis that the NIT was "an electronic tool or technique designed and executed for the purpose of tracking the movement of information both within and outside the Eastern District of Virginia." *Jean*, 2016 WL 4771096, at *13. In determining that the NIT warrant fell within Rule 41(b)(4) authority, Judge Brooks examined *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013), a case also cited by Defendant to support his argument that Judge Buchanan exceeded her authority by issuing the NIT warrant. *Jean*, 2016 WL 4771096, at *13-14. Judge Brooks noted factual differences between the *In re Warrant* case and the circumstances surrounding the NIT warrant, particularly that the malware protocol deployed only after a registered user affirmatively accessed Website A and logged into it and the extent of information obtained from the two malware protocols. *Jean*, 2016 WL 4771096, at *14. Like Judge Brooks, the Court finds the factual differences between this case and *In re Warrant* too great to render it persuasive when reaching a decision here.

Here, Defendant completely discounted the possible application of Rule 41(b)(4), instead focusing solely on Rule 41(b)(1). However, as Judge Brooks reasoned:

> Internet crime and surveillance defy traditional notions of place. An individual may commit the crime of knowingly receiving child pornography without ever having visited the physical location of the server containing these images. All acts are committed over the virtual highways of the internet. And while advances in technology always seem to outpace the abilities of rules committees to keep up, that doesn't necessarily mean that the newer techniques used here were outside the bounds of Rule 41(b), as presently defined.
>
> It is true that the FBI was not seeking to install a tangible tracking device to some other physical piece of property, but Rule 41(b)(4) is not constrained or limited to traditional tracking techniques. Applying the definitions in Rule 41(a)(2), a "tracking device" is any "electronic or mechanical device which permits the

tracking of the movement of a person or object." And subpart (b)(4) authorizes the tracking of "property," which is specifically defined to include the tracking of mere intangible "information." *See* Rule 41(a)(2)(A). Although the term "device" is not more specifically defined in the Rule, it is a word commonly used to describe "a tool or technique used to do a task." Device, American Heritage Dictionary, http://www.yourdictionary.com/device#americanheritage (last visited September 12, 2016).

Here, the government was essentially seeking authority to conduct a sting operation, whereby it would re-launch [Website A] from its own server in Virginia, after which the FBI would then monitor the flow of electronic information as [Website A] users accessed the website for allegedly unlawful purposes. Upon entering this "watering hole," a user—while still immersed—would become infected with the malware as it was deployed to the user's computer incident to the process of downloading child pornography.

Looking to the express language of the warrant application before Judge Buchanan, it was explained that the purpose of the NIT was to secure proof of "the actual location and identity of [Website A] users." [Doc. # 31-1, ¶ 31]. When a [Website A] user accessed the website's content, the NIT electronically "augment[ed]" that content with "additional computer instructions." [*Id.* at ¶ 33]. These instructions caused the user's activating computer to electronically transmit certain identifying information to a computer controlled by the government. [*Id.* at ¶ 34]. As explained above, the simplicity of the NIT was that it caused this information to be transmitted back to the government over the regular internet—thus circumventing TOR's encryption—which in turn allowed the government to track the user's true IP address.

After considering the reasoning []by the various district courts to have considered Judge Buchanan's authority to issue the warrant in question, this Court is persuaded that the investigative technique comports with Rule 41(b)(4)'s tracking exception. First, the NIT is an "electronic device" within the meaning of 18 U.S.C. § 3117(b), because it is an investigative tool consisting of computer code transmitted electronically over the internet. Second, the purpose of the NIT was to track the movement of "property"—which in this case consisted of intangible "information," something expressly contemplated by the definition in Rule 41(a)(2)(A).

The third requirement is that the device be "install[ed]" within the issuing district. As reflected in many of the opinions addressing Judge Buchanan's warrant, the term "install" is problematic, primarily because—in a more traditional scenario—the tracking of tangible property under Rule 41(b)(4) requires the tracking device to be physically attached within the warrant issuing district. But the investigative technique used here was not designed or intended to track a tangible item of physical property. Rather, the NIT was designed to track the flow of intangible property—information—something expressly contemplated by Rule 41(a)(2)(A).

> So when one uses an intangible technique to track the flow of information, to what does the term "install" refer, and where does "installation" take place? . . . While it is obviously true that [Defendant] and his computer were never physically present in Virginia, it is equally accurate that the warrant did not violate Rule 41(b)(4)'s jurisdictional boundaries, because law enforcement did not leave the Eastern District of Virginia to attach the tracking device used here.
>
> The whole point of seeking authority to use a tracking device is because law enforcement does not know where a crime suspect—or evidence of his crime—may be located. In such instances, Rule 41(b)(4) allows a magistrate judge to authorize law enforcement's use of electronic tracking tools and techniques. When an unknown crime suspect, or unknown evidence of his crime, is located in an unknown district, it would be nonsensical to interpret the Rule . . . to require law enforcement to make application for such a warrant to an unknown magistrate judge in the unknown district. The fact that the NIT was purposely designed to allow the FBI to electronically trace the activating computer by causing it to return location identifying information from outside the Eastern District of Virginia—is not only authorized by Rule 41(b)(4), but is the very purpose intended by the exception.
>
> The warrant application alleged that unknown [Website A] users would likely access the website server located in Virginia for purposes of engaging in illegal activity. The application sought authority to track the flow of electronic information while these suspected crimes were occurring. It is undisputed that the NIT authorized by the warrant was executed by the FBI from its computer located within the Eastern District of Virginia. It is also undisputed that but for [Defendant] electronically traveling in search of child pornography to the watering hole in Virginia, the NIT could not have been deployed. Thus, on the facts of this case, the only reasonable interpretation of where the information-tracking NIT was "install[ed]" for purposes of Rule 41(b)(4), is the Eastern District of Virginia, where the tracking device—in this case a string of computer code—was caused to be executed and deployed. The only alternative reading of the Rule would require a finding that magistrate judges do not currently possess authority to issue information-tracking warrants; but such a reading is squarely contradicted by the plain language of Rule 41(a)(2)(A).

Jean, 2016 WL 4771096, at *15-17 (footnotes omitted). This Court agrees with Judge Brooks's analysis and finds "that Rule 41(b)(4) is applicable, that Judge Buchanan possessed the authority to issue the warrant on that basis, and that the resulting seizure of evidence was not unlawful." *Id.* at *17.

B. Suppression of Evidence

However, even if Judge Buchanan issued the NIT warrant in violation of Rule 41(b), suppression of the evidence is not justified. To this end, the Court generally agrees with Judge Maughmer's discussion on pages 7-15 of the R&R. As Judge Maughmer noted, the Eighth Circuit recognizes two types of Rule 41 violations: fundamental and non-fundamental. *United States v. Freeman*, 897 F.2d 346, 350 (8th Cir. 1990). For purposes of possible suppression of evidence, the distinction is critical:

> Only a fundamental violation of Rule 41 requires automatic suppression, and a violation is fundamental only where it, in effect, renders the search unconstitutional under traditional fourth amendment standards. Violations of Rule 41 which do not arise to constitutional error are classified as non-fundamental. Non-fundamental noncompliance with Rule 41 requires suppression only where: (1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule.

Id. (citations omitted).

1. Fundamental Violation

As discussed above, and further elaborated by Judge Maughmer, the alleged violation of Rule 41 does not offend traditional Fourth Amendment standards.

> To demonstrate that the violation of Rule 41 was of constitutional magnitude, [Defendant] must articulate how the government's failure to comply with Rule 41(b) caused a search or seizure prohibited by the Fourth Amendment. In that regard, [Defendant] argues that the Fourth Amendment protects his use of his computer inside the privacy of his own home and, by extension, his identifying IP address.
>
> The Supreme Court of the United States has "uniformly . . . held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by the government action." *Smith v. Maryland*, 442 U.S. 735, 740, 99 S. Ct. 2577, 2580 (1979). That inquiry is analyzed in two parts: (1) whether the individual, through his conduct, "exhibited an actual (subjective) expectation of privacy;" and (2) whether the individual's subjective

expectation of privacy is "one that society is prepared to recognize as 'reasonable." *Id.* (citations omitted).

While the government argues both parts of the analysis are lacking in this case, the Court concludes that [Defendant] did exhibit an actual subjective expectation of privacy in his IP address. His use of the Tor network evidences a clear and unmistakable intent by [Defendant] to mask his identity in general and his IP address in particular. *But see United States v. Stults*, 575 F.3d 834, 842 (9th Cir. 2009) (no subjective expectation of privacy in an IP address since it was shared with and known to a third-party provider).

With regard to whether [Defendant's] subjective desire to maintain his Internet anonymity is one that society is prepared to accept as reasonable, the question is thornier. Certainly, society as a whole does not believe that patrons and promoters of child pornography should be free to traipse around the Internet like some invisible Peeping Tom. On the other hand, society might well accept that there are other instances and situations where cyber-anonymity is both important and reasonable.

An instructive case on the issue is *United States v. Stanley*, 753 F.3d 114 (3d Cir. 2014). In *Stanley*, the criminal defendant accessed his neighbor's wireless Internet connection without permission to share child pornography with other individuals. Police officers eventually learned the defendant's IP address by analyzing the neighbor's Internet router and thereafter locating the defendant by using a device known as a "MoocherHunter" – a mobile tracking software that uses a directional antenna to locate a "mooching computer" by detecting the strength of the radio waves it is emitting. *Id.* at 116. The defendant contended that the use of the MoocherHunter constituted a warrantless search of his property and sought suppression of the evidence against him. *Id.* at 117. Both the district court and the Third Circuit found that the officers did not conduct a "search" within the meaning of the Fourth Amendment because the defendant did not have a reasonable expectation of privacy in his wireless internet signal. *Id.* at 119–22.

The Third Circuit reasoned that "while [the defendant] may have justifiably expected the path of his invisible radio waves to go undetected, society would not consider this expectation 'legitimate' given the unauthorized nature of his transmission." *Id.* at 120. *See also United States v. Jacobson*, 466 U.S. 109, 122, 104 S. Ct. 1652, 1661 (1984) ("The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities."). Specifically, the *Stanley* court concluded that society would be unwilling to recognize the defendant's privacy interests as "reasonable" where "the purpose of [his] unauthorized connection was to share child pornography." *Stanley*, 753 F.3d at 121.

> While acknowledging the closeness of the call, the Court follows the reasoning of the Third Circuit in *Stanley* and district courts like *Werdene* and finds that [Defendant] did not have a reasonable expectation of privacy in his IP address because [Defendant's] subjective expectation of privacy simply is one that society is not prepared to recognize as reasonable. As such, the NIT warrant did not authorize an extra-territorial "search" within the meaning of the Fourth Amendment and the violation of Rule 41 at issue herein is therefore not constitutional, or more precisely, fundamental. Therefore, automatic suppression is not required.

(R&R, pp. 7-9).

2. Non-Fundamental Violation

Defendant alternatively argues suppression is warranted as a non-fundamental violation of Rule 41. (Doc. # 26 pp. 5-6). "[S]uppression of the fruits of the search is not required absent a showing of (1) prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) evidence of intentional and deliberate disregard of a provision in the Rule." *United States v. Burgard*, 551 F.2d 190, 193 (8th Cir. 1977). Despite Defendant's objections to the R&R, the briefs on the Motion to Suppress reveal that Judge Maughmer correctly stated that Defendant only argued for the first factor—prejudice—and did not argue that the officers applying for and executing the NIT warrant acted with intentional or deliberate disregard of the provisions of Rule 41. (*See* Docs. ## 26, 33, 43). Judge Maughmer summarized the parties' arguments on and analyzed the issue as follows:

> [Defendant's] argument for prejudice[5] is straightforward – "the government's violation of Rule 41(b) was uniquely prejudicial because the search of [Defendant's] computer could not have occurred without the void Virginia warrant." Both [Defendant's] argument and the government's counter-argument depend on the meaning of the Eighth Circuit language "the search would not have occurred . . . if the Rule had been followed." In this case, [Defendant] argues that the language means the search could not have occurred at all because the Virginia court – if it had followed Rule 41 – could never have issued a warrant reaching [Defendant] in Missouri. On the other hand, the government argues that *Burgard*

[5] The Court agrees with Judge Maughmer that the burden is on Defendant to demonstrate prejudice. *See, e.g., United States v. Nichols*, 344 F.3d 793, 799 (8th Cir. 2003).

language means that suppression is unjustified if "the evidence contained from a warrant that violates Rule 41(b) could have been available by other lawful means" because "if so, the defendant did not suffer prejudice." *United States v. Vasser*, 648 F.2d 507, 511 (9th Cir. 1980).

Again, although a close call, the Court determines that [Defendant] has not shown prejudice sufficient to warrant suppression. The Eighth Circuit has rejected suppression based on lack of prejudice in other cases involving non-fundamental violations of Rule 41, albeit cases involving more traditionally procedural Rule 41 violations. *See, e.g., United States v. Adams*, 401 F.3d 886, 893 (8th Cir. 2005) (prejudice not proven where officers failed to provide comprehensive inventory of evidence seized during search of defendant's residence); *United States v. Nichols*, 344 F.3d 793, 799 (8th Cir. 2003) (even where search warrant inventory list is deficient, defendant cannot demonstrate prejudice and suppression is not required); *United States v. Sigillito*, 759 F.3d 913, 925 (8th Cir. 2014) (failure to leave attachment to the search warrant at the scene did not warrant exclusion).

[Defendant] argues these cases involved mere technical flaws whereas the warrant in this case was void *ab initio*.[6] The Eighth Circuit cases, however, do not make such a distinction and the Court will not read in such a refinement to the law absent direction from the Eighth Circuit. An instructive case is *United States v. Daughenbaugh*, 5 F.3d 532 [Table], 1993 WL 349400, slip op. (8th Cir. Sept. 8, 1993). In *Daughenbaugh*, a defendant sought to suppress evidence obtained from a search of his cabin, which uncovered processed marijuana, marijuana plants, and several weapons. Before the district court and, later, on appeal, the defendant argued that the government violated FED. R. CRIM. P. 41(a) by obtaining the warrant from a Benton, Arkansas, Municipal Court judge, because the Benton Municipal Court was not a "state court of record" within the meaning of Rule 41. *Id.* at *1. The district court rejected the defendant's argument, determining:

> [In making] the decision to obtain the warrant from the Municipal Court judge, [the officer] had not acted in bad faith and [the defendant] had not suffered any unfair prejudice because the state judge issued the warrant.

Id. On appeal, the Eighth Circuit affirmed the district court, simply noting that the defendant was not "prejudiced by the fact that [the officer] obtained the warrant from the Benton Municipal Court judge." *Id.* at *2. *See also Freeman*, 897 F.2d at 350 (no prejudice to a defendant even though "the person who applied for and participated in the execution of the warrant lacked authority to do so under both federal and state law"). In both *Freeman* and *Daughenbaugh*, the Eighth Circuit did not determine prejudice based on the fact that an underlying warrant may have been invalid at its inception.

[6] While Judge Maughmer stated that the NIT warrant was void *ab initio*, the Court does not agree for all of the reasons contained in this decision.

(R&R, pp. 9-12 (second footnote added)).

C. Good Faith Exception

Alternatively, Judge Maughmer concluded that suppression is not an appropriate remedy for the alleged violation of Rule 41 under the "good faith" exception outlined in *Leon*. The Court agrees the good faith exception applies and adopts the R&R's following discussion:

> When the government seeks to admit evidence collected pursuant to an illegal search or seizure, the judge-created exclusionary rule generally operates to suppress that evidence and makes it unavailable for use at trial. *Herring v. United States*, 555 U.S. 135, 139, 129 S. Ct. 695, 699 (2009). Originally, the exclusionary rule was developed "[t]o deter Fourth Amendment violations." *Id.* Nonetheless, whether suppression is appropriate under the exclusionary rule is a separate question from whether a defendant's Fourth Amendment rights were violated. *Hudson v. Michigan*, 547 U.S. 586, 591-92, 126 S. Ct. 2159, 2164 (2006). Exclusion of unconstitutionally gathered evidence is not a personal right conferred by the Constitution and was not "designed to redress the injury occasioned by an unconstitutional search." *Davis v. United States*, 564 U.S. 229, 236, 131 S. Ct. 2419, 2426 (2011). The fact that a Fourth Amendment violation occurs does not mean that the evidence is automatically suppressed. *Herring*, 555 U.S. at 140, 129 S. Ct. at 700. Instead "exclusion has always been our last resort, not our first impulse." *Id.*
>
> It is well settled that application of the exclusionary rule is "limited to those unusual cases in which it may achieve its objective: to appreciably deter governmental violations of the Fourth Amendment." *Leon*, 468 U.S. at 909, 104 S.Ct. at 3413. "Real deterrent value" alone, however, is insufficient for the exclusionary rule to apply. *Davis*, 564 U.S. at 237, 131 S. Ct. at 2427. The deterrent value must also outweigh the "substantial social costs" of exclusion. *Leon*, 468 U.S. at 907, 104 S. Ct. at 3412. Such costs "often include omitting 'reliable, trustworthy evidence' of a defendant's guilt, thereby 'suppressing the truth and set[ting] [a] criminal loose in the community without punishment.'" *Davis*, 564 U.S. at 237, 131 S. Ct. at 2427. Because such a result runs contrary to the truth-finding functions of judge and jury, exclusion is warranted only where the deterrent value of suppression outweighs the resulting social costs. *Id.*
>
> Against this backdrop, the "good faith" exception to the exclusionary rule was developed to effectuate a balance and has been applied "across a range of cases." *Id.* at 238, 131 S. Ct. at 2427. *Leon* and its progeny highlight that "the deterrence benefits of exclusion 'var[y] with the culpability of the law enforcement conduct' at issue." *Id.* The deterrent value of suppression tends to outweigh the costs "[w]here officers exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard

for Fourth Amendment rights." *Id.* Thus, discerning whether the good faith exception applies requires a court to answer the objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal in light of all of the circumstances. *Herring*, 555 U.S. at 145, 129 S.Ct. at 703.

Leon stands for the proposition that even when a warrant is invalid, if officers reasonably and in good faith relied on the search warrant, then evidence obtained from the search should not be suppressed; instead, "suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule." *Leon*, 468 U.S. at 918, 104 S. Ct. at 3418. In this case, the Court concludes that the officers applying for and executing the Virginia NIT warrant reasonably and in good faith relied on the warrant. As such, the Court concludes that that even if the analysis set out in the first part of this Report and Recommendation is in error—and the Fourth Amendment and/or Rule 41[7]—were indeed violated, suppression of the evidence obtained against [Defendant] pursuant to the Virginia NIT warrant still should not be ordered. As found by the Supreme Court:

> The deterrent purpose of the exclusionary rule necessarily assumes that the police have engaged in willful, or at the very least negligent, conduct which has deprived the defendant of some right. By refusing to admit evidence gained as a result of such conduct, the courts hope to instill in those particular investigating officers, or in their future counterparts, a greater degree of care toward the rights of an accused. Where the official action was pursued in complete good faith, however, the deterrence rationale loses much of its force. . . . If the purpose of the exclusionary rule is to deter

[7] Typically, the application of *Leon* occurs in cases where the Fourth Amendment has been violated and the defendant seeks suppression based on the judicially-created exclusionary rule. In this case, the Court would also apply *Leon* to a violation of Rule 41. It would make no sense to find a good faith exception to suppression for a Constitutional violation, but refuse to apply such an exception to a violation of a procedural rule. *Compare United States v. Calandra*, 414 U.S. 338, 348 n.6, 94 S. Ct. 613, 619 n.6 (1974) (Federal Rules of Criminal Procedure do "not constitute a statutory expansion of the exclusionary rule").

> [The defendant] has not directed the court's attention to any Eighth Circuit cases holding Rule 41(d) is violated [under the facts of the case]. However, even assuming arguendo that the Eighth Circuit would reach a similar result and find a Rule 41(d) violation occurred, suppression still may not be warranted based on the good faith exception to the exclusionary rule set forth in [*Leon*].

United States v. Spencer, 2004 WL 1834627, op. at *10–11 (N.D. Iowa Aug. 11, 2004), *aff'd*, 439 F.3d 905 (8th Cir. 2006).

> unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment.
>
> *United States v. Peltier*, 422 U.S. 531, 539, 542, 95 S. Ct. 2313, 2318, 2320 (1975).

(R&R, pp. 12-15).

CONCLUSION

The Court adopts the R&R as noted in its discussion above. Additionally, Defendant did not have a reasonable expectation of privacy in his IP address and the NIT warrant is valid. Accordingly, for these reasons and the reasons stated above, Defendant's Motion to Suppress Evidence is DENIED.

IT IS SO ORDERED.

s/ Gary A. Fenner
GARY A. FENNER, JUDGE
UNITED STATES DISTRICT COURT

DATED: October 20, 2016